REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 4-6, and 8-18 are pending in the present application, Claims 1, 4, and 12-18 having been amended. Support for the amendments to Claims 1, 4, and 12-18 is found, for example, in Figs. 1 and 4, and in the specification at page 11, lines 15-24 and page 19, line 20 to page 20, line 10. Thus, no new matter is added.

In the outstanding Office Action, Claims 11, 4-6, and 8-18 were rejected under 35 U.S.C. §112, second paragraph; Claims 1-, 4-6, 8, 9, 11, and 14-18 were rejected under 35 U.S.C. §102(b) as anticipated by Delayaye et al. (U.S. Patent No. 4,751,733, hereinafter Delayaye); and Claims 10, 12, and 13 were rejected under 35 U.S.C. §103(a) as unpatentable over Delayaye in view of Matsui et al. (U.S. Patent No. 6,201,869, hereinafter Matsui).

With respect to the rejection of Claims 1, 4-6, and 8-18 under 35 U.S.C. §112, second paragraph, Claims 1, 4-6, and 8-18 are amended to more clearly describe and distinctly claim the subject matter regarded by the Applicants as the invention.

As shown in Fig. 1 of the present application, for a non-limiting embodiment of the claimed invention, each of a plurality of parallel nonlinear transformation modules 2 (extended S-boxes) in each stage executes local, lower-level diffusion, a diffusion module 3 (a higher-level MDS) executes broad, higher-level diffusion over the block width, the non-linear transformation modules 2 execute local, lower-level diffusions. This process is repeated at a predetermined number of stages.[1]

Further, as shown in Fig. 4 and discusses on page 19, line 20 to page 20, line 10 of the present specification, each of the extended S-boxes 103 diffuses 32-bit data and each of the higher-level MDS diffusion layers 104-1 to 104-8 diffuses 128-bit data.

[1] Specification, page 11, lines 15-24.

Accordingly, Claims 1, 4, 12, 13, 14, 15, 16, 17, and 18 are amended to more clearly describe how data is diffused with respect to a size.

The outstanding Office Action takes the position that claim language "to connect as least one input bit terminal of the first units to one input bit terminal of the corresponding first unit...via at least two paths" is indefinite because it appears inconsistent with the remarks in the response filed on August 29, 2005. Applicants respectfully offer the following comments to clarify the comments provided in the response filed August 29, 2005.

In a non-limiting embodiment of the claimed invention, Fig. 35 shows one input bit terminal 1001 of a first unit 103 connected to one input bit terminal 1002 of a corresponding first unit in the succeeding encryption section via at least two paths. Thus, in the non-limiting embodiment of Fig. 35, 1001 represents an input bit terminal, and not the first unit. Accordingly, Applicants respectfully submit that the claim language is correct and clearly describes and distinctly claims the subject matter regarded by the Applicants as the invention.

Thus, Applicants respectfully submit that Claims 1, 4, 5, 6, 12, 13, and 16 comply with the requirements of 35 U.S.C. §112, second paragraph.

Furthermore, the antecedent basis informalities identified in Claims 12 and 13 are corrected by the present amendment.

With respect to the rejection of Claims 14, 15, 17, and 18, which recites "repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is reflected on one bit input to the next randomizing operation via at least two paths," the outstanding Office Action appears to take the position that Claims 14, 15, 17, and 18 are indefinite because the term "reflected" is vague. Applicants have amended Claims 14, 15, 17, and 18 to recite "repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation is transmitted to the next randomizing operation via at least two paths."

Accordingly, Applicants respectfully submit that Claims 14, 15, 17, and 18 comply with the requirements of 35 U.S.C. §112, second paragraph.

If, however, the Examiner disagrees, the Examiner is invited to telephone the undersigned who will be happy to work with the Examiner in a joint effort to derive mutually satisfactory claim language.

In a non-limiting embodiment of the claimed invention, nested (recursive) SPN encryption includes a combination of local randomization (lower-level diffusion) and diffusion over a block width (higher-level diffusion). As shown in Fig. 1, each of the parallel nonlinear transformation modules (extended S-boxes) 2 in each stage executes local, lower-level diffusion. Diffusion module (a higher-level MDS) 3 executes broad, high-level diffusion over the block width. Each nonlinear transformation module 3 is constructed by alternately arranging nonlinear transformation modules (S-boxes) and diffusion modules (lower-level MDS). That is, in the nested SPN structure, lower-level SPN structures (two stages of SPN structures) are recursively embedded in S-box portions of the normal SPN structure.[2]

In the non-limiting embodiment of the claimed invention, the security of the nested (recursive) SPN encryption against SQUARE attack is higher than SQUARE encryption/Rijndael encryption because of randomizing by the higher-level MDS diffusion layer provided between S-boxes (between the second-half S-boxes of the preceding (or the last) extended S-box and the first-half S-boxes of the succeeding (or the first) extended S-box).[3]

SQUARE attack on SPN encryption follows a procedure of inputting 256 patterns (Λ set) that satisfies conditions: (1) variable bytes take 256 patterns, and (2) other bytes are fixed

[2] Specification, page 10, lines 23-26, and page 11, lines 15-24.
[3] Specification, page 47, line 24 to page 48, line 6.

and searching for a key for which the bit sum for 256 patterns becomes zero, thereby estimating the key.[4]

The security against SQUARE attack is improved by adding given conditions to the combination in the higher-level MDS (the combination relationship among input and output bits of the higher-level MDS or the interconnect relationship among operational paths). The given conditions double or multiply all or part of the differential paths (operational paths between the first half of S-boxes of the preceding extended S-box and the first half S-boxes of the succeeding extended S-box). Thus, a high avalanche effect is achieved and the number of stages that are subject to SQUARE attack are reduced.[5]

Turning now to the rejection of independent Claim 1 as anticipated by Delayaye, Applicants respectfully traverse the rejection. Claim 1 is amended to recite, *inter alia*, "wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths." Delayaye does not teach or suggest at least this element of amended Claim 1.

Delayaye does not disclose the above-described doubling or multiplication of all or part of differential paths. Delayaye does not disclose or suggest that the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths, as recited in Claim 1.

Figs. 5 and 6 of Delayaye show wiring diagrams used to perform permutation operations. As shown in Figs. 5 and 6, each bit is only connected to one other bit via one path.

[4] Specification, page 48, lines 7-12.
[5] Specification, page 48, lines 13-26.

Furthermore, Matsui does not teach or suggest "wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths." Matsui only describes a nonlinear transformer 131 including a Galois Field inverse circuit 152.[6] Matsui does not teach or suggest nested (recursive) SPN encryption including a combination of local randomization (lower-level diffusion) and diffusion over the block width (higher-level diffusion).

In view of the above noted distinctions, Applicants respectfully submit that Claim 1 patentably distinguishes over Delayaye and Matsui, alone or in combination. In addition, independent Claims 4 and 12-18 recite elements similar to the elements of Claim 1. Thus, Applicants respectfully submit that Claims 4, and 12-18 (and Claims 5, 6, 8 and 9-11) patentably distinguish over Delayaye and Matsui, alone or in combination.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
I:\ATTY\JW\210580US\210580US_AM DUE 4-28-06.DOC

[6] Matsui, Fig. 2.